Performance Pack

NGX (R60A)

IMPORTANT

Check Point recommends that customers stay up-to-date with the latest service packs and versions of security products, as they contain security enhancements and protection against new and changing attacks.

CHECK POINT SECUREKNOWLEDGE DATABASE

For additional technical information about Check Point products, consult Check Point's SecureKnowledge at:
https://secureknowledge.checkpoint.com

See the latest version of this document in the User Center at:

http://www.checkpoint.com/support/technical/documents/docs_R60.html

Intelligent Security

September 2005

We Secure the Internet.

Check Point Software Technologies Ltd.

U.S. Headquarters: 800 Bridge Parkway, Redwood City, CA 94065, Tel: (650) 628-2000 Fax: (650) 654-4233, info@CheckPoint.com

International Headquarters: 3A Jabotinsky Street, Ramat Gan, 52520, Israel, Tel: 972-3-753 4555 Fax: 972-3-575 9256, http://www.checkpoint.com

2000, 2001, 2002 Philip Warner. Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs. Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@graphviz.org). Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@graphviz.org). Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information. Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande. Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation. This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation. This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation. Although their code does not appear in gd 2.0.4, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

The curl license

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2004, Daniel Stenberg, <daniel@haxx.se>.All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose

with or without fee is hereby granted, provided that the above copyright

notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

The PHP License, version 3.0

Copyright (c) 1999 - 2004 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP, freely available from <http://www.php.net/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group. The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <http://www.php.net>. This product includes the Zend Engine, freely available at <http://www.zend.com>.

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright (c) 2003, Itai Tzur <itzur@actcom.co.il>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Neither the name of Itai Tzur nor the names of other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

U.S. Government Restricted Rights

The material in document is provided with "RESTRICTED RIGHTS." Software and accompanying documentation are provided to the U.S. government ("Government") in a transaction subject to the Federal Acquisition Regulations with Restricted Rights. The Government's rights to use, modify, reproduce, release, perform, display or disclose are restricted by paragraph (b)(3) of the Rights in Noncommercial Computer Software and Noncommercial Computer Soft-ware Documentation clause at DFAR 252.227-7014 (Jun 1995), and the other restrictions and terms in paragraph (g)(3)(i) of Rights in Data-General clause at FAR 52.227-14, Alternative III (Jun 87) and paragraph (c)(2) of the Commer-cial

Computer Software-Restricted Rights clause at FAR 52.227-19 (Jun 1987).

Use of the material in this document by the Government constitutes acknowledgment of NextHop's proprietary rights in them, or that of the original creator. The Contractor/ Licensor is NextHop located at 1911 Landings Drive, Mountain View, California 94043. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in applicable laws and regulations.

Disclaimer Warranty Disclaimer Warranty Disclaimer Warranty Disclaimer Warranty

THE MATERIAL IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT POSSIBLE PURSUANT TO THE APPLICABLE LAW, NEXTHOP DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON INFRINGEMENT OR OTHER VIOLATION OF RIGHTS. NEITHER NEXTHOP NOR ANY OTHER PROVIDER OR DEVELOPER OF MATERIAL CONTAINED IN THIS DOCUMENT WARRANTS OR MAKES ANY REPRESEN-TATIONS REGARDING THE USE, VALIDITY, ACCURACY, OR RELIABILITY OF, OR THE RESULTS OF THE USE OF, OR OTHERWISE RESPECTING, THE MATERIAL IN THIS DOCUMENT.

Limitation of Liability

UNDER NO CIRCUMSTANCES SHALL NEXTHOP BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR PROFIT, ARISING OUT OF THE USE, OR THE INABILITY TO USE, THE MATERIAL IN THIS DOCUMENT, EVEN IF NEXTHOP OR A NEXTHOP AUTHORIZED REPRESENTATIVE HAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IF YOUR USE OF MATERIAL FROM THIS DOCUMENT RESULTS IN THE NEED FOR SERVICING, REPAIR OR CORRECTION OF EQUIPMENT OR DATA, YOU ASSUME ANY COSTS THEREOF. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT FULLY APPLY TO YOU.

BIND: ISC Bind (Copyright (c) 2004 by Internet Systems Consortium, Inc. ("ISC"))

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language. Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Table Of Contents

CHAPTER 1

Introduction to Performance Pack

In This Chapter

Overview

This document describes how to install and configure Performance Pack. Additionally, it shows you how to get the best possible performance using Performance Pack.

Performance Pack is supported both for SecurePlatform and Solaris platforms. Performance Pack is a software acceleration product installed as an add-on to VPN-1 Pro. Performance Pack significantly enhances and improves the performance of VPN-1 Pro.

Performance Pack uses Check Point's SecureXL technology and other innovative network acceleration techniques, to deliver wire-speed performance for VPN-1 Pro. Moreover, it accelerates key security functions, thereby ensuring your organization the best security with the best performance available on an open platform.

Supported security functions include:

- Access control.
- Encryption.
- NAT.
- Accounting and logging.
- Connection/session rate.
- General security checks.

- SmartDefense features.
- CIFs resources.
- ClusterXL High Availability and Load Sharing.
- TCP Sequence Verification.
- Dynamic VPN

Release Notes

The latest Release Notes for Performance Pack can be found at:

http://www.checkpoint.com/support/technical/documents/index.html

CHAPTER 2

Getting Started

In This Chapter

Performance Pack NGX System Requirements

Performance Pack accelerates the performance of VPN-1 Pro on Pentium PCs supported by SecurePlatform, on Solaris 8, or Solaris 9 SPARC 64 Bit.

Following are the minimum recommended requirements:

Minimum System Requirements

The following are the minimum system requirements:

TABLE 2-1 Minimum System Requirements

Operating Systems	SecurePlatform NGX (R60A) Solaris 8, Solaris 9.
CPU	Pentium III and above for SecurePlatform NGX (R60A). SPARC 64 Bits for Solaris.
Disk Space	80 MB.
Memory	128 MB.

TABLE 2-1 Minimum System Requirements

Network Interfaces	Network Interfaces supported by VPN-1 Pro on Solaris: ▪ GEM Ethernet NIC. ▪ 10/100 QuadEthernet NIC. ▪ GigaSwift NIC. ▪ Sun HME 10/100 Ethernet NIC. ▪ BGE

Recommended System Options

The following system options are recommended for optimal performance:

TABLE 2-2 Recommended System options

Operating Systems	SecurePlatform NGX (R60A), Solaris 8, Solaris 9.
CPU	Dual Intel Xeon or Dual SPARC 64 bits
Disk Space	400 MB.
Memory	512 MB or more.
Network Interfaces	SecurePlatform NGX (R60A): Intel Pro 1000 MF/MT. Solaris: GigaSwift.
Bus Technology	At least two 64bit/66Mhz PCI buses, ServerWorks or Intel E7500 Chipset.

Performance Pack Recommended Platforms

The following platforms are recommended for use with Performance Pack:

- Super Micro SuperServer 6023P-8R Dual Processor.
- Compaq ML530 Dual Processor.
- Compaq Proliant Dual Processor.
- IBM 330, 340 & 343 Dual Processor.
- Dell precision 530 Dual Processor.
- SunBlade 1000.
- SunFire V480.
- SunFire V210/V240

Please refer to the latest Performance Pack NGX (R60A) release notes for additional information on hardware support, limitations and recommendations.

Preparing the Performance Pack Machine

For optimal performance, appropriate configuration settings are recommended for the following:

- BIOS Settings.
- Network Interface Cards.

BIOS settings

- If your BIOS supports CPU clock setting, make sure that the BIOS is set to the actual CPU speed.
- If you are running Performance Pack NGX (R60A) on a machine with Intel Xeon CPUs, consider setting the HyperThreading feature to "on". Using HyperThreading may improve performance for some scenarios.

Network Interface Cards location

- If you are using a motherboard with multiple PCI or PCI-X buses, make sure that each Network Interface Card is installed in a slot connected to a *different* bus.
- If you are using more than two Network Interface Cards in a system with only two 64bit/66Mhz PCI buses, make sure that the least-used cards are installed in slots connected to the *same* bus.

Note - Performance Pack is automatically disabled on PPTP and PPPoE interfaces.

Installation

For installation details see the most current online documentation:

http://www.checkpoint.com/support/technical/documents/

CHAPTER 3

Command Line

In This Chapter

fwaccel

The `fwaccel` utility allows you to enable or disable acceleration dynamically while VPN-1 Pro is running. The default setting is determined by the setting configured with cpconfig (see `cpconfig` on page 14). This setting reverts to the default after reboot.

Usage

```
fwaccel [on|off|stat|stats|conns|templates]
```

Parameters

TABLE 3-1 fwaccel parameters

Parameter	Explanation
`on`	Start acceleration.
`off`	Stop acceleration.
`stat`	Display the acceleration device status and the status of the Connection Templates on the local VPN-1 Pro module.
`stats`	Displays acceleration statistics.

TABLE 3-1 fwaccel parameters

Parameter	Explanation
`stats -s`	Displays more summarized statistics information.
`conns`	Displays all connections.
`conns -s`	Displays the number of connections currently defined in the accelerator.
`templates`	Display all connection templates.
`templates -max_entries`	Display up to max_entries connection templates.
`templates -s`	Display the number of templates currently defined in the accelerator.

cpconfig

Check Point products are configured using the `cpconfig` utility. When run, this utility displays a screen with the configuration options. The options that are displayed, depend on the installed configuration and product(s). You can use `cpconfig` to enable or disable Performance Pack. Once you have selected an acceleration setting, the setting remains configured, until you choose to change it on another occasion. In other words, the settings that you define will remain even after the machine is rebooted. For an alternative method to enable or disable acceleration, see "fwaccel" on page 15.

Usage

Execute cpconfig by entering the following command:

```
cpconfig
```

An interactive menu will be displayed providing you with the option to enable or disable the acceleration by selecting `Enable/Disable Check Point SecureXL`. Select `Enable` in order to enable acceleration. Select `Disable` in order to disable acceleration.

sim

The `sim` utility controls various Performance Pack NGX R60A driver features and applies only for SecurePlatform.

Usage

```
sim affinity [-a|-s|-l]
```

Parameters

Affinity is a general term for binding Network Interface Card (NIC) interrupts to processors. By default, SecurePlatform does not set Affinity to the NIC interrupts, which means that each NIC is handled by all processors. Optimal network performance is obtained when each NIC is individually bound to a single processor. To achieve the above, the `sim` utility includes an Affinity feature, which has the following operation modes:

TABLE 3-2 sim Affinity operation modes

Option	Explanation
`-a`	**Automatic Mode** — the Affinity is determined automatically, by analyzing the load on each NIC. If the NICs are not loaded, the Affinity will not be set. This is the default Affinity operation mode, in which the Affinity is re-tuned every 60 seconds.
`-s`	**Manual Mode** — allows you to manually specify the Affinity settings. For each interface, you will be asked to enter one of the following: • A space-separated list of the processor numbers that are to handle this interface, *or* • The word `all`, to allow all processors to handle this interface. When setting the Affinity manually, the periodic automatic check will be disabled. After booting, it will remain disabled and the Affinity settings entered manually will be applied.
`-l`	View a list of the current Affinity settings.

proc entries

Performance Pack supports SecurePlatform `proc` entries. These entries are used to display information about the Performance Pack.

The proc entries are read-only entries. They cannot be configured. The proc entries are located under `/proc/ppk`.

Usage

```
cat /proc/ppk/[conf|ifs|statistics]
```

Parameters

TABLE 3-3 /proc Parameters

Parameter	Explanation
`conf`	Displays the Performance Pack Configuration.
`ifs`	Lists the interfaces to which Performance Pack is attached.
`statistics`	Displays general Performance Pack statistics.

Appendix **A**

Performance Tuning and Measurement Hints

In This Appendix

Performance Tuning

SYN Defender

To obtain optimal TCP connection setup rate performance, verify that the SYN Defender method specified in the SmartDefense is set to **None** (default).

Amount of Concurrent Connections and Hash Size

Setting the Maximal Concurrent Connections

To set the desired number of maximal concurrent connections, open SmartDashboard's **Gateway Object Properties** window and proceed as follows:

1. Open the **Capacity Optimization** tab. Make sure that **Calculate connections hash table size and memory pool** is set to **Automatically**.
2. Set the desired amount of concurrent connections in the **Maximum Concurrent Connections** field.

Increasing the Number of Concurrent Connections

You can increase the actual number of concurrent connections by reducing the timeout of TCP and UDP sessions:

- TCP end timeout determines the amount of time a TCP connection will stay in the FireWall connection table after a TCP session has ended.
- UDP virtual session timeout determines the amount of time a UDP connection will stay in the FireWall connection table after the last UDP packet was seen by the gateway.

By reducing the above values, the capacity of actual TCP and UDP connections is increased.

Implied Rules

In order to set the optimal connection/sec rate, proceed as follows:

1. Select **Global Properties** from the **Policy** menu.
2. Select **FireWall-1** in the **Global Properties** tree.
3. *Uncheck* the following options:
   - **Accept RIP**
   - **Accept Domain Name over UDP (Queries)**
   - **Accept Domain Name over TCP (Zone Transfer)**
   - **Accept ICMP requests**

HyperThreading

HyperThreading applies only to SecurePlatform.

HyperThreading is a feature of some Intel processors that enables emulation of two virtual processors by a single physical processor. This feature increases the performance under certain conditions.

Machines with Xeon processors have a BIOS option that may allow enabling or disabling HyperThreading, under the following circumstances:

- If the number of network interfaces is less than the actual physical number of processors (i.e. two network interfaces and three processors), it is recommended to *enable* HyperThreading.
- If the number of network interfaces is equal to or greater than the actual physical number of processors (i.e. two network interfaces and two processors), it is recommended to disable HyperThreading.
- If cryptography is used extensively, HyperThreading should be enabled.

Connection Templates

General

Connection templates are generated from active connections according to the policy rules. The connection template feature accelerates the speed at which a connection is established by matching a new connection to a set of attributes. When a new connection matches the template, connections are established without performing a rule match and therefore are accelerated. Connection templates are generated from active connections according to policy rules. Currently, connection template acceleration is performed only on connections with the same destination port.

Examples:

- A connection from 10.0.0.1/2000 to 11.0.0.1/80 — established through Firewall and then accelerated.
- A connection from 10.0.0.1/2001 to 11.0.0.1/80 — fully accelerated (including connection establishment).
- A connection from 10.0.0.1/8000 to 11.0.0.1/80 — fully accelerated (including connection establishment).

HTTP GET requests to specific server will be accelerated since the connection has the same source IP address.

Restrictions

In general, Connections Templates will be created only for plain UDP or TCP connections. The following restrictions apply for Connection Template generation:

Global restrictions:

- SYN Defender — Connection Templates for TCP connections will not be created.
- NAT connections.
- VPN connections.
- Complex connections (H323, FTP, SQL).
- NetQuotas.
- ISN Spoofing.

If the Rule Base contains a rule regarding one of the following component, the Connection Templates will be disabled for connections matching this rule, and for all of the following rules:

- Security Server connections.
- Services with source port range.
- Time objects in the rules.

- Dynamic Objects and/or Domain Objects.
- Services of type "other" with a match expression.
- User/Client/Session Authentication actions.
- Services of type RPC/DCERPC/DCOM.

When installing a policy containing restricted rules, you will receive console messages indicating that Connection Templates will not be created due to the rules that have been defined. The warnings should be used as a recommendation that will assist you to fine-tune your policy in order to optimize performance.

Testing

To verify that connection templates are enabled, use the `fwaccel stat` command. To verify that connection templates are generated, use `fwaccel templates`. This should be done while traffic is running, in order to obtain a list of currently defined templates.

Delayed Synchronization

The synchronization mechanism guarantees High Availability. In a cluster configuration, if one cluster member fails, the other recognizes the connection failure and takes over, so the user does not experience any connectivity issue. However, there is an overhead per synchronized operation, which can occasionally cause a system slow-down when there are short sessions.

Delayed synchronization is a mechanism based upon the duration of the connection, with the duration itself used to determine whether or not to perform synchronization. A time range can be defined per service. The time range indicates that connections terminated before a specified expiration time will not be synchronized. As a result, synchronized traffic is reduced and overall performance increases. Delayed Synchronization is performed only for connections matching a connection template.

Configuration

Currently, delayed synchronization is allowed only for services of type HTTP or None. In order to configure delayed synchronization, proceed as follows:

1. In SmartDashboard, right click on the **Service** tab.
2. Either edit an existing service or click **New** and select **TCP**. The **TCP service properties** window is shown.
3. After defining TCP parameters, click **Advanced** in the **TCP service properties** window. The **Advanced TCP Service Properties** window is shown.
4. Select the **HTTP** or **None** protocol from the **Protocol Type** list.

5 Check **Start synchronizing**.

6 Define the duration value **Seconds after connection initiation**. The duration value is specified in seconds.

Performance Measurement

TCP State and Benchmarking

Certain testing applications (SmartBits or Chariot) generate invalid TCP sequences. The VPN-1 Pro module's TCP state check detects these faulty sequences, and drops the packets. As a result, the benchmark fails. Since these TCP sequences are invalid, they may affect overall Firewall performance.

To disable this type of TCP state check, perform the following operations on the SmartCenter Server:

1 Select the **Smart Defense** tab in the SmartDashboard.

2 Click the **TCP** object under Network Security.

3 In the **TCP** window, disable **Sequence Verifier**.

4 Install the Policy from SmartDashboard in order to apply the changes.

Index